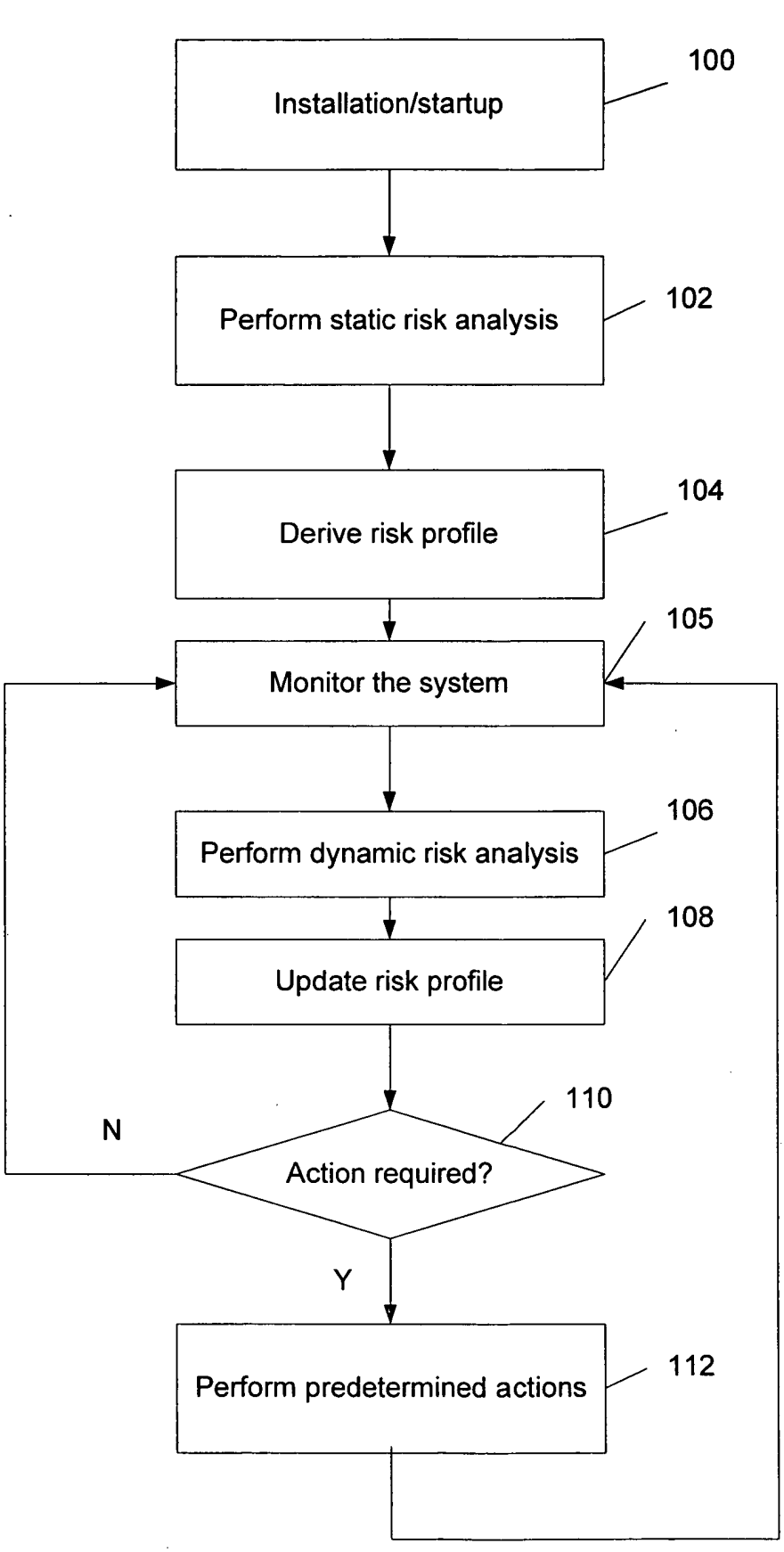
120
Installation/startup
100
Perform static risk analysis
102
Derive risk profile
104
Monitor the system
105
Perform dynamic risk analysis
106
Update risk profile
108
Action required?
110
N
Y
Perform predetermined actions
112

Figure 1

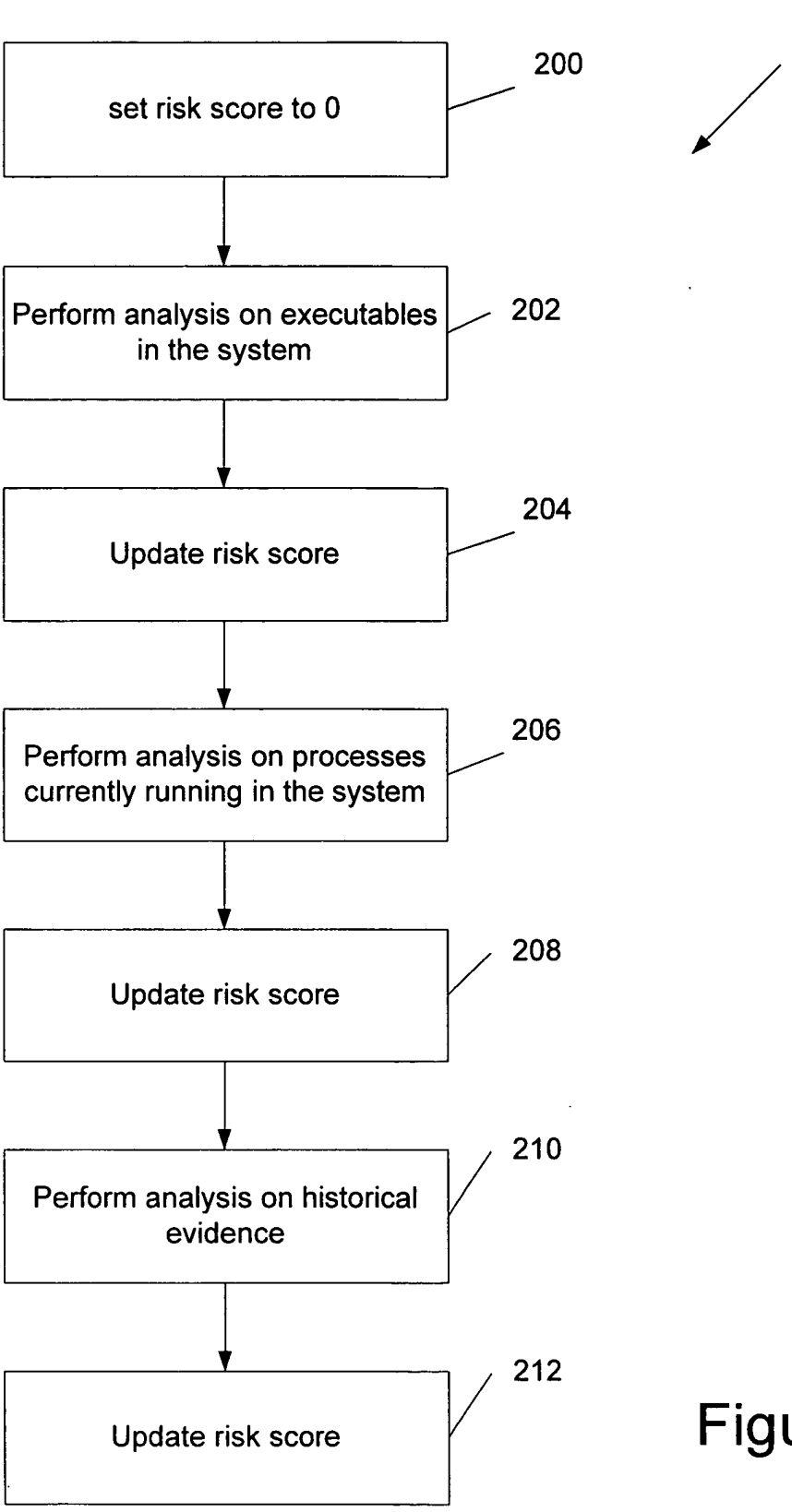
102
set risk score to 0
200
Perform analysis on executables in the system
202
Update risk score
204
Perform analysis on processes currently running in the system
206
Update risk score
208
Perform analysis on historical evidence
210
Update risk score
212

Figure 2

Subcategories	Criteria used to analyze executables	Risk value
Configuration	runs as a service	1
	runs under highly privileged account	1
	is not installed via a standard procedure	2
	has insufficient access control	1
	is recent	1
	is not signed	1
	modified date is not the same as created date	1
Capabilities	has networking capability	2
	has privilege manipulation capabilities	1
	has remote process capabilities	1
	can launch other processes	1
Misc. properties	has secure coding violations	1

Figure 3

Subcategories	Criteria used to analyze running processes	Risk value
Configuration	has higher effective privilege	1
	has more privileges than the process should have	1
	has loaded in extra dynamic libraries	1
Capabilities	owns system objects that do not have sufficient access control	1
	owns UDP port (sending)	1.5
	owns UDP port (listening)	2
	owns TCP port (sending)	0.5
	owns TCP port (listening)	1

Figure 4

Run-time analysis criteria	Risk value
launches child processes without complete path specification	1
launches child processes that inherit privileges	1
exhibits different attributes/behavior given different arguments	1
impersonates users	1

Figure 5